

In re Patent Application of
LIARDET ET AL.
Serial No. 09/506,158
Filed: FEBRUARY 17, 2000

In the Claims:

Claims 1-10 (Cancelled).

11. (Currently amended) An electronic circuit for the securing of a cryptography coprocessor comprising:

a memory module for storing a message to be processed by an encryption or decryption operation and a an unencrypted digital key;

a battery of input/output registers connected to the memory module by a first two-way link for receiving digital key data from said memory module comprising the unencrypted digital key and a plurality of scrambling bits intermixed with the unencrypted digital key;

said battery of input/output registers comprising a scrambling register for storing the scrambling bits separate from the unencrypted digital key data;

an input register for receiving the message to be processed;

a key register for receiving the unencrypted digital key data for use in the encryption or decryption operation;

a multiplexer to carry out a transfer of data between the battery of input/output registers and the input register and the key register;

a second, dedicated two-way link connecting said multiplexer and said scrambling register for transferring the scrambling bits therebetween substantially simultaneously with the transfer of data between the battery of input/output

In re Patent Application of
LIARDET ET AL.
Serial No. 09/506,158
Filed: **FEBRUARY 17, 2000**

registers and said multiplexer; and

a processing module connected to said scrambling register, said input register, and said key register for determining the unencrypted digital key based upon the digital key data in said key register and the scrambling bits in said scrambling register, and for performing the encryption or decryption operation on the message stored in the input register based thereon;

a control module for controlling the memory module, the battery of input/output registers, the multiplexer and the processing module; and

an output register to transmit the result of the encryption or decryption operation to the battery of input/output registers through the multiplexer.

12. (Previously presented) An electronic circuit according to Claim 11 wherein the scrambling bits are foreign to the message to be processed and to the digital key.

13. (Previously presented) An electronic circuit according to Claim 11, further comprising an accessory input register connected between said processing module and said scrambling register to receive the scrambling bits.

14. (Previously presented) An electronic circuit according to Claim 13, wherein the accessory input register is the same size as the scrambling register.

In re Patent Application of
LIARDET ET AL.
Serial No. 09/506,158
Filed: FEBRUARY 17, 2000

15. (Previously presented) An electronic circuit according to Claim 11, wherein the scrambling bits are generated randomly.

16. (Previously presented) An electronic circuit according to Claim 11, wherein the scrambling bits are sent in groups of eight bits.

17. (Currently amended) An electronic circuit for a cryptography coprocessor comprising:

a plurality of input/output registers having a scrambling register for receiving digital key data comprising a an unencrypted digital key and a plurality of scrambling bits intermixed with the unencrypted digital key;

an input register for receiving message data to be processed by the encryption or decryption operation;

a key register for receiving the digital key data for use in the encryption or decryption operation;

a multiplexer for transferring data between the plurality of input/output registers and the input register and the key register;

a dedicated two-way link connecting said multiplexer and said scrambling register for transferring the scrambling bits therebetween substantially simultaneously with the transfer of data between the battery of input/output registers and said multiplexer; and

a processor connected to said scrambling register, said input register, and said key register for performing the

In re Patent Application of
LIARDET ET AL.
Serial No. 09/506,158
Filed: **FEBRUARY 17, 2000**

encryption or decryption operation on the message data in the input register based upon the digital key data and the scrambling bits;

 a controller for controlling the plurality of input/output registers, the multiplexer and the processor; and
 an output register to transmit the result of the encryption or decryption operation to the plurality of input/output registers through the multiplexer.

18. (Previously presented) An electronic circuit according to Claim 17 wherein the scrambling bits are foreign to the message data and the digital key.

19. (Previously presented) An electronic circuit according to Claim 17, further comprising an accessory input register connected between said processor and said scrambling register to receive the scrambling bits.

20. (Previously presented) An electronic circuit according to Claim 19, wherein the accessory input register is the same size as the scrambling register.

21. (Previously presented) An electronic circuit according to Claim 17, further comprising a memory connected to the plurality of input/output registers for storing the message to be processed and the digital key.

22. (Previously presented) An electronic circuit

In re Patent Application of
LIARDET ET AL.
Serial No. 09/506,158
Filed: FEBRUARY 17, 2000

according to Claim 19, wherein the accessory input register is the same size as the scrambling register.

23. (Previously presented) An electronic circuit according to Claim 17, wherein the scrambling bits are generated randomly.

24. (Previously presented) An electronic circuit according to Claim 17, wherein the scrambling bits are sent in groups of eight bits.

25. (Currently amended) A method for securing a cryptography coprocessor comprising:

transmitting data by a first two-way link from a memory module to a battery of input/output registers, the battery of input/output registers comprising a scrambling register;

transmitting data corresponding to a message to be processed by an encryption or decryption operation, through a multiplexer, from the battery of input/output registers to an input register; and

transmitting digital key data for the encryption or decryption operation comprising a an unencrypted digital key and a plurality of scrambling bits intermixed with the digital key, through the multiplexer, from the battery of input/output registers to a key register while substantially simultaneously transferring the scrambling bits between the multiplexer and the scrambling register via a second, dedicated two-way communication link, and storing the scrambling bits, which are foreign to the

In re Patent Application of
LIARDET ET AL.
Serial No. 09/506,158
Filed: FEBRUARY 17, 2000

message to be processed and the unencrypted digital key, in the scrambling register of the battery of input/output registers;

using a processing module to determine the unencrypted digital key based upon the digital key data stored in the key register and the scrambling bits stored in the scrambling register; and

performing the encryption or decryption operation on the message to be processed stored in the input register with the processing module based upon the determined digital key, and outputting the result of the encryption or decryption operation to an output register.

Claim 26 (canceled).

27. (Previously presented) A method according to Claim 25, wherein the scrambling bits are randomly intermixed with the digital key.

28. (Previously presented) A method according to Claim 25, wherein the scrambling bits are transmitted to the scrambling register whenever digital key data is input into the battery of input/output registers.

29. (Previously presented) A method according to Claim 25, wherein the scrambling bits comprise groups of eight bits.

30. (Currently amended) A method for operating a cryptography coprocessor comprising:

In re Patent Application of
LIARDET ET AL.
Serial No. 09/506,158
Filed: **FEBRUARY 17, 2000**

transmitting data to a plurality of input/output registers, the plurality of input/output registers comprising a scrambling register;

transmitting message data to be processed by an encryption or decryption operation, through a multiplexer, from the plurality of input/output registers to an input register; and

transmitting digital key data for the encryption or decryption operation comprising a an unencrypted digital key and a plurality of scrambling bits intermixed with the digital key, through the multiplexer, from the plurality of input/output registers to a key register while substantially simultaneously transferring the scrambling bits between the multiplexer and the scrambling register via a dedicated two-way link, and storing the scrambling bits in the scrambling register of the plurality of input/output registers; and

processing the message data with a processor receiving the data from the input register, receiving the digital key data from the key register, and the scrambling bits from the scrambling register, and outputting the corresponding message data to an output register.

Claim 31 (canceled).

32. (Previously presented) A method according to Claim 30, wherein the scrambling bits are intermixed with the digital key randomly.

33. (Previously presented) A method according to Claim

In re Patent Application of
LIARDET ET AL.
Serial No. 09/506,158
Filed: **FEBRUARY 17, 2000**

/

30, wherein the scrambling bits are transmitted to the scrambling register whenever digital key data is input into the plurality of input/output registers.

34. (Previously presented) A method according to Claim 30, wherein the scrambling bits comprise groups of eight bits.